UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/771,840	02/04/2004	Art Shelest	MSFT121932	9753

26389 7590 12/23/2008
CHRISTENSEN, O'CONNOR, JOHNSON, KINDNESS, PLLC
1420 FIFTH AVENUE
SUITE 2800
SEATTLE, WA 98101-2347

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
12/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/771,840	SHELEST ET AL.	
	Examiner	Art Unit	
	JUNG KIM	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 October 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10,12,14,15,17-23,25-45,47-51,53,56 and 60-63* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10,12,14,15,17-23,25-45,47-51,53,56 and 60-63* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office action is in response to the RCE filed on 10/16/08.

2. Claims 1-10, 12, 14, 15, 17-23, 25-45, 47-51, 53, 56 and 60-63 are pending.

Continued Examination Under 37 CFR 1.114

3. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10/16/08 has been entered.

Response to Arguments

4. Applicant's arguments have been fully considered but they are not persuasive.

5. With respect to Applicant's arguments that neither Sobel nor Herrmann discloses "a clean group that is managed by a domain controller configured to store information identifying network users and resources," (Remarks, pgs. 15 and 16) this argument is not persuasive because Sobel expressly discloses a DHCP proxy intercepts access requests to determine if a user is compliant and forwards the access request to a DHCP server, which channels a user's access to either a protected network or a restricted network (paragraphs 25 and 26); moreover, a DHCP server necessarily contains

information about client configuration parameters, default gateway, and other servers. Herrmann discloses a NAS incorporating a filter which permits a client to connect, but subject to constraints or conditions depending on the compliance test results for the client; this filter may define session access for the user to a limited group of IP address. (paragraph 97) Hence, contrary to Applicant's arguments, both Sobel and Herrmann suggest "a clean group that is managed by a domain controller configured to store information identifying network users and resources."

6. With respect to Applicant's arguments that Sobel fails to teach that the clean group server rather than the compliance verification component resident on the client determines whether an item has a specified set of properties (Remarks, pg. 16), it is noted that claims 1 and 33 are worded such that the step of evaluating client data to determine compliance is not necessarily performed by the clean group server. Claim 1 merely requires that the clean group server determines from the evidence in the add request whether the item has the specified set of properties. Claim 33 is similarly worded. These limitations only require that the evidence allow the clean group server to determine if the item has the specified properties or not. Hence, Applicant's arguments for claims 1 and 33 are insufficient because they are based on limitations not recited in the claims. With respect to claims 15 and 26, Applicant's arguments are moot in view of the new rejections. (Claims 15 and 26 are distinguished from claims 1 and 33, as claims 15 and 26 define that the clean group server determines if the add request contains "sufficient" evidence to prove the item has the specified set of properties)

Applicant's conclusionary statement that Herrmann and Lineman similarly fail to disclose these features (Remarks, pg. 17, first paragraph, last sentence) is an insufficient basis to overcome a prima facie case of evidence. Conclusionary statements, by themselves, do not establish a rationale or argument against a 103(a) rejection because they are merely statements; nor do they provide any factual support for a claim that a rejection based on the combined teachings of two references does not properly render the claimed invention obvious. Furthermore, contrary to applicant's statement, as noted in the rejections, Herrmann explicitly discloses that the clean group server evaluates the evidence to determine if there is "sufficient" evidence to prove whether an item has a specified set of properties. See below.

7. Finally, Applicant's arguments that none of the prior art discloses that clean group membership of a user is evaluated on the basis of whether each of a set of computers associated with the user is in compliance (Remarks, pg. 17) is not persuasive because in the prior art (Sobel, Herrmann and Lineman), each user is associated with a computer; a computer defines a set. Hence, the prior art suggest that membership of a user is evaluated on the basis of whether each of a set of computers associated with the user is in compliance.

8. Applicant's remaining arguments are cumulative to those discussed above. Hence, for these reasons, claims 1-10, 12, 14, 15, 17-23, 25-45, 47-51, 53, 56 and 60-63 remain rejected.

Claim Rejections - 35 USC § 112

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claim 17 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

11. Claim 17 recites the limitation "items". There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

12. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

13. Claims 1-9, 12, 14, 33-38, 60, 62 and 63 are rejected under 35 USC 102(e) as being anticipated by Sobel et al. US Patent Application Publication No. 20040103310 (hereinafter Sobel).

14. As per claims 1-9 and 12, 14, 60, 62 and 63, Sobel discloses a method for providing security in a computer system by a clean group server, comprising:

a. specifying a set of properties for use in determining if an item is clean (paragraph 20);

b. in response to receiving an add request from an item, the add request containing evidence collected from the item relating to the presence or absence of the properties in the specified set of properties, evaluating the add request to determine if the evidence proves that the item has the specified set of properties (paragraphs 24-26, if 325 the requesting client 105 is compliant with the security policies, the DHCP proxy 110 requests 330 an IP address from the DHCP server 150 on the protected network 140"; Compliance Registration Manager and DHCP Proxy are functionally equivalent to the limitation "clean group server");

c. determining from the evidence in the add request whether the item has the specified set of properties, and if so, designating the item as a member of a clean group by instructing a domain controller to add the item to the clean group, the domain controller configured to store information identifying network users and resources (paragraphs 24 and 25; DHCP server 150 on the protected side);

d. wherein the item is a computer (paragraph 13);

e. wherein when the computer is to be evaluated, a clean component is installed on the computer to perform compliance checks and to collect the evidence relating to the presence or absence of the properties in the specified set of properties (paragraphs 19-20, compliance verification component 190);

f. wherein a compliance check is performed at a selected time for an item to determine if the item has the specified set of properties (paragraph 20 and 24);

g. wherein one of the specified set of properties is whether all of the available updates have been installed (paragraph 17);

h. wherein the updates comprise at least one of security updates or service packs (paragraph 17);

i. further comprising receiving a message sent by the clean component after the item fails a compliance check performed by the clean component, wherein the message indicates that the item should not be in the clean group; (paragraphs 21 and 24)

j. further comprising invalidating the clean group membership of the item in response to receiving the message (paragraphs 21 and 24-27);

k. wherein invalidating the clean group membership of the item comprises local actions including at least hiding the domain credentials of the item. (paragraph 25; item is segregated into a restricted network)

l. wherein after the item is designated as a member of the clean group, a countdown is started and if another message is not received by the end of the countdown, the item is removed from the clean group (paragraph 25; a timeout feature is inherent in connection oriented communications);

m. further comprising initiating a status check to determine if the items in the clean group still have the specified properties (paragraph 20);

n. further comprising designating the item as a member of a dirty group if the clean group server determines that the item does not have the specified set of properties (paragraph 26, client is assigned to restricted network);

o. wherein the invalidating the clean group membership of the item comprises local actions including at least erasing the domain credentials of the item; (paragraphs 20, 27, 33)

p. wherein if the compliance check fails, additional steps are taken including at least logging out a privileged user. (paragraphs 20, 27, 33)

15. As per claims 33-38, Sobel discloses a method for providing security in a computer system, comprising:

q. Specifying a set of properties for use in determining if a computer is clean (paragraph 12);

r. Evaluating a computer to determine if it has the specified set of properties;

s. Sending an add request to a clean group server (paragraphs 22-24); and

t. based on whether or not the clean group server determines that the computer is in compliance, the clean group server disabling or enabling the computer domain account on a domain controller, the domain controller configured to store information identifying network users and resources; (paragraph 24-26; DHCP proxy and server)

u. wherein when a new computer domain account is to be added to the domain, the new domain account is placed in a disabled state until the associated computer is proved to the clean group server to be in compliance; (paragraph 29)

v. wherein when a new computer domain account is to be added to the domain, the domain join operation that creates the new computer domain account is predicated on proving that the computer is in compliance by requiring the clean group server to participate in the domain join operations; (paragraph 21)

w. wherein evaluating a computer comprises determining whether available updates have been installed on the computer (paragraph 14);

x. wherein the computer periodically performs compliance checks; (paragraphs 20 and 24)

y. wherein the clean group server periodically initiates a compliance check on the computer (paragraphs 20 and 24).

Claim Rejections - 35 USC § 103

16. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

17. Claim 10 is rejected under 35 USC 103(a) as being unpatentable over Sobel.

18. As per claim 10, the rejection of claim 7 under 35 USC 102(e) as being anticipated by Sobel is incorporated herein. Sobel further discloses that if the compliance check fails, the client is not given access to the protected network.

(paragraph 26) The inability to access resources on the protected network disables the client from connecting with these resources via any secure connections using standard techniques such as SSL or VPN. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to hide cryptographic keys if the compliance check fails because the client is denied access to these resources. The aforementioned cover the limitations of claim 10.

19. Claims 15, 17-23, 25-32, 61 are rejected under 35 USC 103(a) as being unpatentable over Sobel in view of Ide et al. US 7,162,649 (hereinafter Ide)

20. As per claims 15, 17-21, 25 and 61, Sobel discloses a system for managing security, comprising:

z. A clean group server; (fig. 1, Compliance Registration Manager and DHCP Proxy are functionally equivalent to the limitation "clean group server)

aa. A domain controller configured to store information identifying network users and resources, including a clean group indicating a group of computers that are more trusted than computers not included in the clean group (paragraph 25, DHCP server; computers and users are separated between protected network and restricted network);

bb. a clean runtime component, the clean runtime component being installed on an item and being able to communicate with the clean group server (paragraph 19 and 20, compliance verification component);

cc. the clean runtime component configured to send an add request to the clean group server, the add request including evidence to be evaluated by the clean group server for determining whether to add the item to a clean group (paragraph 24);

dd. wherein the clean group server is configured to determine from the evidence whether the item is in compliance with a security policy, and if so. to designate the item as a member of the clean group by instructing the domain controller to add the item to the clean group (paragraphs 24 and 25; DHCP server 150 on the protected side);

ee. wherein the items comprise computers (paragraph 13);

ff. wherein the clean runtime component is configured to perform self-governance compliance checks to determine if the item meets selected criteria; (paragraphs 20 and 24)

gg. wherein one of the criteria is whether selected available updates have been installed; (paragraph 17)

hh. wherein the updates comprise at least one of security updates or service packs; (paragraph 17)

ii. wherein the clean runtime component is configured to, if a self-governance compliance check performed by the clean runtime component fails, send a message from the clean runtime component to the clean group server to indicate that the item should not be in the clean group; (paragraphs 21 and 24)

jj. wherein the clean group server is configured to initiate a compliance check for items to determine if they should remain in the clean group; (paragraph 20)

21. Sobel does not disclose wherein a clean group comprises a group of computers and users; adding the computer as a member of a clean group if the clean group server determines that the add request contains sufficient evidence to prove that the computer has the specified set of properties; wherein the clean group server is further configured to designate the item as a member of a dirty group if the evidence sent by the clean runtime component is insufficient to prove that the item is in compliance with the security policy. Ide discloses an apparatus for network assessment and authentication, wherein when a user's credential and computer are checked for compliance before a user is allowed access to the service. Ide discloses two embodiments of the same concept: in one, a user performs a self-check and generates an assessment of their workstation, whereby the user sends the workstation assessment as well as the user credentials to access a network service (Col. 7:41-8:14); In a different embodiment, Ide discloses when a user requests access to a network service, the user provides both their user credentials and computer credentials to either the network server which includes the network service or a separate server, which includes a workstation assessment service ,whereupon either the network server or the separate server generates a vulnerability assessment based on the received computer credentials (Col. 7:1-30; 8:44-50; 9:33-38); moreover, if either the user credentials or the computer credentials are found to be insufficient, then access to the service can be restricted.

Col. 7:30-42 (degraded level of service or deny access if the credentials do not satisfy the workstation security policy). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made wherein a clean group comprises a group of computers and users; adding the computer as a member of a clean group if the clean group server determines that the add request contains sufficient evidence to prove that the computer has the specified set of properties; wherein the clean group server is further configured to designate the item as a member of a dirty group if the evidence sent by the clean runtime component is insufficient to prove that the item is in compliance with the security policy. One would be motivated to do so to ensure that the users are properly authenticated; and to centralize assessment of workstation compliance so that the system does not have to rely on the trusted state of localized assessment services as known to one of ordinary skill in the art. The aforementioned cover the limitations of claims 15, 17-21, 25 and 61.

22. As per claim 22, the rejection of claim 18 under 35 USC 103(a) as being unpatentable over Sobel in view of Ide is incorporated herein. Although neither Sobel nor Ide expressly disclose wherein the clean runtime component is configured to send the add request to the clean group server only after the self-governance compliance check passes, Such a feature would be obvious to one of ordinary skill in the art. In both Sobel and Ide, the inventions disclose embodiments where the client performs self-governance compliance check. Supra. A determination that the local workstation is not compliant by a service resident in the workstation enables the user to know the status of

their workstation at that point. There is no further need to submit an add request if it is determined that the workstation is not compliant. The motivation for submitting an add request only if the self-governance compliance check passes would be to reduce the add request traffic to the clean group server as known to one of ordinary skill in the art. Official notice is taken of this teaching. The aforementioned cover the limitations of claim 22.

23. As per claim 23, the rejection of claim 15 under 35 USC 103(a) as being unpatentable over Sobel in view of Ide is incorporated herein. Although Sobel does not disclose the limitation wherein the clean group server is configured to, after designating the item as a member of the clean group, start a countdown; and if another add request is not received by the end of the countdown, the clean group server is configured to remove the item from the clean group; such a feature is well established in many technological fields, including provisioning of user accounts by network service providers, etc. Timeout features for stored registration values are a common technique to weed out obsolete values; without such a mechanism, obsolete values would persist forever. Hence, timeout procedures maintain an efficient allocation of resources for active uses only. Official notice of this teaching is taken. Therefore, it would be obvious to one of ordinary skill in the art wherein the clean group server is configured to, after designating the item as a member of the clean group, start a countdown; and if another add request is not received by the end of the countdown, the clean group server is

configured to remove the item from the clean group. The aforementioned cover the limitations of claim 23.

24. As per claims 26-32, Sobel discloses one or more computer-readable media having computer-executable components for providing security in a computer system, the computer-executable components (paragraph 5) comprising:

kk. a clean runtime object for installation on a computer, wherein the clean runtime object, when executed, performs a compliance check to determine if the computer has a specified set of properties, and sends an add request containing evidence relating to whether the computer has the specified set of properties to a clean group server; (paragraphs 19-21)

ll. instructions for installation on a clean group server for processing the add request, wherein the instructions, when executed, cause the clean group server to instruct a domain controller configured to store information identifying network users and resources to add the computer as a member of a clean group upon receipt of an add request, if the clean group server determines that the add request contains evidence to prove that the computer has the specified set of properties; (paragraphs 24-26)

mm. wherein the compliance check is performed initially upon installation of the runtime object; (paragraph 19)

nn. wherein the evidence indicates whether specified available updates have been installed on the computer; (paragraph 17)

oo. wherein the specified available updates comprise at least one of security updates or service packs; (paragraph 17)

pp. wherein after the add request is received by the clean group server, a countdown is started and if another message is not received by the end of the countdown, the clean group server instructs the domain controller to remove the computer from the clean group; (paragraph 25; a timeout feature is inherent in connection oriented communications)

qq. wherein the clean runtime object initiates a compliance check on the computer (paragraph 20);

rr. wherein the clean group server communicates with the runtime object to initiate a compliance check (paragraphs 19 and 20).

25. Sobel does not disclose adding the computer as a member of a clean group if the clean group server determines that the add request contains sufficient evidence to prove that the computer has the specified set of properties. Ide discloses an apparatus for network assessment and authentication, wherein when a user's credential and computer are checked for compliance before a user is allowed access to the service. Ide discloses two embodiments of the same concept: In one, a user performs a self-check and generates an assessment of their workstation, whereby the user sends the workstation assessment as well as the user credentials to access a network service (Col. 7:41-8:14). In a different embodiment, Ide discloses when a user requests access to a network service, the user provides both their user credentials and computer credentials to either the network server which includes the network service or a

separate server, which includes a workstation assessment service ,whereupon either the network server or the separate server generates a vulnerability assessment based on the received computer credentials (Col. 7:1-30; 8:44-50; 9:33-38); moreover, if either the user credentials or the computer credentials are found to be insufficient, then access to the service can be restricted. Col. 7:30-42 (degraded level of service or deny access if the credentials do not satisfy the workstation security policy). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to add the computer as a member of a clean group if the clean group server determines that the add request contains sufficient evidence to prove that the computer has the specified set of properties. One would be motivated to do so to ensure that the users are properly authenticated; and to centralize assessment of workstation compliance so that the system does not have to rely on the trusted state of localized assessment services as known to one of ordinary skill in the art. The aforementioned cover the limitations of claims 26-32.

26. Claims 39-45, 47, 51, 53 and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sobel in view of Lineman et al. US Patent Application Publication No. 20030065942 (hereinafter Lineman).

27. As per claims 39-45, 47, 51 and 53, Sobel discloses a method for providing security in a computer system comprising:

ss. performing compliance checks for items; placing items which pass the compliance check into a clean group by communicating with a domain controller, the domain controller configured to store information identifying network users and resources; and removing items from the clean group which fail the compliance check; (Abstract; paragraphs 12; 25 and 26, DHCP proxy and server)

tt. wherein the item is a computer; (paragraph 13)

uu. wherein the item performs a compliance check; (paragraphs 20 and 24)

vv. wherein a clean group server initiates a compliance check on the item; (paragraphs 20 and 24)

ww. wherein the compliance check is performed by the item communicating with an update Web site to determine if updates are available for the item; (paragraphs 14 and 17)

xx. wherein the item communicates with a clean group server to establish its membership in the clean group; (fig. 1, reference nos. 110, 115, 120, 125, 130, 135)

yy. wherein a compliance check is initiated by one or more of a client coming online, changes in client status/configuration, changes in network status/configuration, or changes to a compliance policy; (fig. 3; paragraph 20)

zz. wherein an item is a user, and a user's clean group membership is evaluated on the basis of whether each of a set of computers associated with the user is in compliance. (paragraph 12; one computer defines a set)

28. Although Sobel does not disclose the feature wherein after an item passes a compliance check and is placed in the clean group, a countdown is started and if another compliance check is not passed by the end of the countdown, the item is removed from the clean group; such a feature is well established in many technological fields, including provisioning of user accounts by network service providers, etc. Timeout features for stored registration values are a common technique to weed out obsolete values; without such a mechanism, obsolete values would persist forever. Hence, timeout procedures maintain an efficient allocation of resources for active uses only. Official notice of this teaching is taken. Therefore, it would be obvious to one of ordinary skill in the art wherein after an item passes a compliance check and is placed in the clean group, a countdown is started and if another compliance check is not passed by the end of the countdown, the item is removed from the clean group.

29. Moreover, Sobel does not disclose wherein the clean group is utilized to provide enforcement of the computer security policy by binding active directory group policy to the group membership such that only members of the group can read the policy; wherein items within the clean group can access a collection of IPSec communication requirements and parameters that allow them to communicate with other items within the clean group; and items not within the clean group cannot access the collection of IPSec communication requirements and parameters, and are thereby quarantined from receiving information from or sending information to items within the clean group. Lineman discloses a method and apparatus for managing security policies, including a common feature to provide limited access to published security policies that include the

following steps: preparing security policy documents and publishing these documents, wherein only specified users with defined roles have access to a particular published document. This feature effectively prevents users who do not have the proper access privileges to read the security policies and thereby prevent unauthorized users from attaining the privileges reserved for specific roles. Paragraph 70. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the invention of Sobel to enforce the computer security policy by binding active directory group policy to the group membership such that only members of the group can read the policy; wherein only computers which comply with the policy and are thus members of the clean group can read the policy parameters and thus communicate with one another, while computers which are not members of the clean group are effectively prevented from communicating with computers in the clean group, thus in effect providing a quarantine mechanism. One would be motivated to do so to significantly enhance the communication of these security policies to the users. Lineman, ibid.

30. Finally, Sobel does not disclose the security policy provides IPSec communication requirements and parameters. However, it is notoriously well known in the art that IPSec communications provides secure communications between a sender and a receiver to ensure that communications are not monitored by an unscrupulous 3rd party. In addition, IPSec protocols operate in the network layer to provider greater flexibility over other secure protocols such as SSL. For example, Microsoft's Active Directory, which provides centralized management and configuration of computers, enables centralized IPsec configuration for secure communications between computers

configured via the Active Directory. Official notice of this teaching is taken. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made for the security policy to provide IPSec communication requirements and parameters. One would be motivated to do so to provide flexible and secure communication between a sender and a receiver. The aforementioned cover the limitations of claims 39-45, 47, 51 and 53.

31. As per claim 56, the rejection of claim 39 under 35 USC 103(a) as being unpatentable over Sobel in view of Lineman is incorporated herein. Sobel does not expressly disclose wherein a client that changes state from membership in the clean group to non-membership is required to clear all policy settings distributed via the clean group. However, it is notoriously well known in the art at the time of invention to invalidate policy settings when a client is no longer part of a group. For example, a user's access credentials, such as passwords and usernames are conventionally deactivated or deleted by an administrator when a user is removed as a client. Official notice of this teaching is taken. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the invention of Sobel to include the step of wherein a client that changes state from membership in the clean group to non-membership is required to clear all policy settings distributed via the clean group. One would be motivated to do so to prevent access by a user whose privileges have been revoked as known to one of ordinary skill in the art. The aforementioned cover the limitations of claim 56.

32. Claims 48-50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sobel in view of Lineman, and further in view of Herrmann et al. US Patent Application 20040107360 (hereinafter Herrmann).

33. As per claims 48 and 49, the rejection of claim 39 under 35 USC 103(a) as being unpatentable over Sobel in view of Lineman is incorporated herein. Sobel does not disclose wherein a clean group server communicates to non-compliant items how to get back into compliance; wherein the non-compliant items are directed to a Web site with online instructions to the user, and once the instructions are followed, another server-assisted compliance check is initiated. Herrmann discloses a method for policy enforcement, whereby when a client device requests access to a protected network service, the client device provides policy information regarding the status of the client's device to a policy server; whereupon the policy server checks the policy information to determine if the client device is compliant. If the device is not compliant, a packet is returned to the client, which may contain a message to be displayed to the user, which can serve as a launching point for remediation; for example, advise the client that he or she can use a web browser to download and install any required software. Once the proper software is installed, the client can re-authenticate with the service. Paragraphs 79 and 97. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made wherein a clean group server communicates to non-compliant items how to get back into compliance; wherein the non-compliant items are directed to

a Web site with online instructions to the user, and once the instructions are followed, another server-assisted compliance check is initiated. One would be motivated to do so for ease of use as known to one of ordinary skill in the art. The aforementioned cover the limitations of claims 48 and 49.

34. As per claim 50, the rejection of claim 48 under 35 USC 103(a) as being unpatentable over Sobel in view of Lineman and Herrmann is incorporated herein. Neither Sobel, Lineman nor Herrmann disclose wherein the non-compliant items are instructed how to get into the compliant state automatically without requiring a user's involvement. However, automation of a step is deemed to be an obvious enhancement. In re Venner, 262 F.2d 91, 95, 120 USPQ 193, 194 (CCPA 1958). It would be obvious to one of ordinary skill in the art at the time of invention to modify the invention of Herrmann to include the feature wherein the non-compliant items are instructed how to get into the compliant state automatically without requiring a user's involvement. One would be motivated to do so to replace the manual activity with an automatic means of making the non-compliant item to be compliant as known to one of ordinary skill in the art. The aforementioned cover the limitations of claim 50.

35. Claims 39, 41-45, 47-51, 53 and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Herrmann in view of Lineman.

36. As per claims 39, 41-45, 47-49, 51 and 53 Herrmann discloses a method for providing security in a computer system, comprising:

aaa. performing compliance checks for items; placing items which pass the compliance check into a clean group by communicating with a domain controller, the domain controller configured to store information identifying network users and resources; and removing items from the clean group which fail the compliance check; (paragraphs 96 and 97; the NAS implements a filter to permit a client to connection subject to constraints depending on the compliance test)

bbb. wherein the item is a computer; (fig. 4, reference no. 310)

ccc. wherein the item performs a compliance check; (paragraph 94)

ddd. wherein a clean group server initiates a compliance check on the item; (paragraphs 93-95)

eee. wherein the compliance check is performed by the item communicating with an update Web site to determine if updates are available for the item; (paragraphs 79 and 97)

fff. wherein the item communicates with a clean group server to establish its membership in the clean group; (paragraph 76-79 and 93-95)

ggg. wherein a compliance check is initiated by one or more of a client coming online, changes in client status/configuration, changes in network status/configuration, or changes to a compliance policy; (fig. 7A, reference no. 701)

hhh. wherein a clean group server communicates to non-compliant items how to get back into compliance; (paragraph 79 and 97)

iii. wherein the non-compliant items are directed to a Web site with online instructions to the user, and once the instructions are followed, another server-assisted compliance check is initiated; (paragraph 79 and 97)

jjj. wherein an item is a user, and a user's clean group membership is evaluated on the basis of whether the each of a set of computers associated with the user is in compliance. (fig. 4, reference no. 310 and related text; one computer defines a set)

37. Herrmann does not disclose wherein the clean group is utilized to provide enforcement of the computer security policy by binding active directory group policy to the group membership such that only members of the group can read the policy; wherein items within the clean group can access a collection of IPSec communication requirements and parameters that allow them to communicate with other items within the clean group; and items not within the clean group cannot access the collection of IPSec communication requirements and parameters, and are thereby quarantined from receiving information from or sending information to items within the clean group. Lineman discloses a method and apparatus for managing security policies, including a common feature to provide limited access to published security policies that include the following steps: preparing security policy documents and publishing these documents, wherein only specified users with defined roles have access to a particular published document. This feature effectively prevents users who do not have the proper access

privileges to read the security policies and thereby prevent unauthorized users from attaining the privileges reserved for specific roles. Paragraph 70. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the invention of Herrmann to enforce the computer security policy by binding active directory group policy to the group membership such that only members of the group can read the policy; wherein only computers which comply with the policy and are thus members of the clean group can read the policy parameters and thus communicate with one another, while computers which are not members of the clean group are effectively prevented from communicating with computers in the clean group, thus in effect providing a quarantine mechanism. One would be motivated to do so to significantly enhance the communication of these security policies to the users. Lineman, ibid.

38. Finally, Herrmann does not disclose the security policy provides IPSec communication requirements and parameters. However, it is notoriously well known in the art that IPSec communications provides secure communications between a sender and a receiver to ensure that communications are not monitored by an unscrupulous 3rd party. In addition, IPSec protocols operate in the network layer to provider greater flexibility over other secure protocols such as SSL. For example, Microsoft's Active Directory, which provides centralized management and configuration of computers, enables centralized IPsec configuration for secure communications between computers configured via the Active Directory. Examiner takes Official notice of this teaching. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made for the security policy to provide IPSec communication requirements and

parameters. One would be motivated to do so to provide flexible and secure communication between a sender and a receiver. The aforementioned cover the limitations of claims 39, 41-49, 51 and 53.

39. As per claim 50, the rejection of claim 48 under 35 USC 102(e) as being anticipated by Herrmann is incorporated herein. Herrmann does not disclose wherein the non-compliant items are instructed how to get into the compliant state automatically without requiring a user's involvement. However, automation of a step is deemed to be an obvious enhancement. In re Venner, 262 F.2d 91, 95, 120 USPQ 193, 194 (CCPA 1958). It would be obvious to one of ordinary skill in the art at the time of invention to modify the invention of Herrmann to include the feature wherein the non-compliant items are instructed how to get into the compliant state automatically without requiring a user's involvement. One would be motivated to do so to replace the manual activity with an automatic means of making the non-compliant item to be compliant as known to one of ordinary skill in the art. The aforementioned cover the limitations of claim 50.

40. As per claim 56, the rejection of claim 39 under 35 USC 103(a) as being unpatentable over Herrmann in view of Lineman is incorporated herein. Herrmann does not expressly disclose wherein a client that changes state from membership in the clean group to non-membership is required to clear all policy settings distributed via the clean group. However, it is notoriously well known in the art at the time the invention was made to invalidate policy settings when a client is no longer part of a group. For

example, users access means, such as passwords and usernames are conventionally deactivated or deleted by an administrator when a user is removed as a client. Examiner takes Official notice of this teaching. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the invention of Herrmann to include the step of wherein a client that changes state from membership in the clean group to non-membership is required to clear all policy settings distributed via the clean group. One would be motivated to do so to prevent access by a user whose privileges have been revoked. The aforementioned cover the limitations of claim 56.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you

have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Jung Kim/
Primary Examiner, AU 2432